**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| **BETSY FEIST, individually and on behalf of all similarly situated,** | ) | |
| **Plaintiff,** | ) | **CASE NO.** |
| **v.** | ) | **11-CV-5436 (LGS)** |
| **PAXFIRE, INC,** | ) | |
| **Defendant** | ) | |

**PLAINTIFF PAXFIRE'S MOTION TO DIMISS COUNT ONE OF DEFENDANT BETSY FEIST'S COMPLAINT OR, IN THE ALTERNATIVE, FOR SANCTIONS FOR DEFENDANT'S SPOLIATION OF ELECTRONICALLY STORED EVIDENCE**

Defendant Paxfire, Inc. ("Paxfire"), through its undersigned attorneys and pursuant to Fed. R. Civ. P. 37(e) and the inherent power of this Court, hereby moves to dismiss Count One of Plaintiff Betsy Feist's ("Ms. Feist") Complaint; or, in the alternative, to impose evidentiary sanctions: excluding at trial or in motions for summary judgment any evidence of, or reference to, Paxfire having intercepted or redirected Ms. Feist's Internet communications as to all her claims.

Ms. Feist willfully destroyed material evidence, specifically records stored on her personal computer of the web pages that she visited and cookies placed there by third parties. This information would have enabled Paxfire to refute Ms. Feist's allegations that it intercepted and redirected her electronic communications. The allegation that Paxfire unlawfully intercepted Ms. Feist's internet communications and redirected her searches is the core of her claim against Paxfire in Count One of her Complaint.

**MEMORANDUM**

Among Ms. Feist's allegations are that Paxfire: (1) unlawfully intercepted her electronic communications; and (2) unlawfully redirected her communications. Specifically, she claims that Paxfire unlawfully intercepted electronic signals that she transmitted to and through her internet service provider ("ISP"), this being the RCN Corporation[1] ("RCN"); and that Paxfire unlawfully disclosed electronic signals that Ms. Feist intended to transmit to third party search engines by redirecting them to internet vendors. The communications and searches are those supposedly originating from her home computer.

Ms. Feist does not allege a mere a scheme—Count One of her Complaint (Doc. 1) alleges that *specific instances* of interception and redirection occurred, each such instance violating the Electronic Communications Privacy Act[2] ("ECPA"). She seeks statutory damages for each instance, plus "actual damages." (Cmpl. ¶¶ 41-48.) To defend against these claims, Paxfire is entitled to try to establish that (1) Paxfire did not intercept any of Ms. Feist's communications; and (2) Paxfire did not redirect any of Ms. Feist's internet searches. Paxfire is also entitled to contest damages, i.e., to identify the number of specific ECPA violations that occurred, if any, so as to limit statutory and other damages. Two pieces of evidence are critical to these endeavors: cookies and Ms. Feist's web browsing history. Both were stored on the hard drive of Ms. Feist's personal computer.

After she filed her lawsuit—which she did on August 4, 2011—and before she produced a copy of her hard drive in discovery, she destroyed this evidence: she "cleaned" the hard drive of her home computer, using a commercially available application. Paxfire is prejudiced by this

[1] The RCN Corporation was initially named as a defendant in this case. Ms. Feist and RCN settled, and the Complaint was dismissed as to RCN. (Doc. 81.)
[2] 18 U.S.C. § 2510 *et seq*.

spoliation, because it lost valuable evidence that to refute Ms. Feist's claims, or, at a minimum, limit the damages that Ms. Feist is seeking. Paxfire seeks an appropriate remedy.

**I. Background: Ms. Feist's Allegations**

Before proceeding further, Paxfire notes that it disputes many of Ms. Feist's allegations, including the most important one—that Paxfire "unlawfully" intercepted any of Ms. Feist's electronic signals. It will, however, leave those factual disputes to resolution through motions for summary judgment and trial.

The pertinent allegations are in paragraphs fourteen through twenty-two of the Complaint, and fall into two categories:

(1) Paxfire intercepted the search terms that internet users enter into a search box provided by search engines (specifically, Google, Bing, and Yahoo![3]), acquiring the electronic signals resulting from those entries by means of a "proxy server" rather than transmitting them directly to the search engines. Ms. Feist alleges that Paxfire's use of a proxy server is somehow an "interception,"[4] and that through this means Paxfire collected and profiled the search histories of internet users, then selling or otherwise distributing these histories for profit.[5]

(2) Appearing on the edges or "bars" of many Internet web browsers are an "address bar" and an additional search box, hereinafter referred to as a "search bar." These typically appear at

[3] Cmpl. ¶ 15.
[4] Cmpl. ¶ 16-17.
[5] Cmpl. ¶ 18. For the sake of background, we note that (a) the use of proxy servers is ubiquitous on the Internet, made necessary to reduce the load of routine internet traffic; and (b) although it used proxy servers, Paxfire ultimately directed any user's request, when entered on a specific search engine's own web page, through its proxy server to that search engine. It did not collect, profile, distribute, or sell any search histories of any user, contrary to the claims made by Ms. Feist. We also note that the electronic transmissions of customers of RCN, of which Ms. Feist was one, that passed through Paxfire's computer servers did so in the ordinary course of RCN's business operations, and thus Paxfire's acquisition of such communications was lawful under the safe harbor provider of 18 U.S.C. § 2510(5)(a)(ii).

the top of a web browser: to the left is the address bar, and to the right is the search bar.[6] Ms. Feist alleges that Paxfire intercepted words typed into the search bars of Internet users, and, instead of transmitting all directly to a search engine, "redirected" certain "keywords" to third party merchants.[7] Ms. Feist alleges that such an interception, taken from the search bar on the web browser (not to be confused with the search box on a search engine's own web page), and the subsequent redirection are violations of ECPA.

When Paxfire was involved in the transmission of an internet user's electronic signals (such occurring when Paxfire was contracted to do so by the user's ISP[8]), Paxfire installed a cookie on the user's machine. The purpose of this cookie was to enable Paxfire to count the number of unique personal computers using its services, so as to obtain a "head count" of users. (Dep. M. Sullivan at 128:6--131:2, 137:15-22, Ex. 12) It did not use such cookies to personally identify users. (*Id*. at 196:3-10.) The appearance of Paxfire's cookie on a user's computer indicated that Paxfire had been involved in the transmission of that user's electronic communications. The absence of Paxfire's cookie on a user's computer indicates that Paxfire was not involved in the transmission of that user's communications.

After a redirection occurred, if one occurred, the user would be directed to the web page of a third-party merchant. For example, if a user entered the word "apple" in his or her search bar, instead of being directed to Google and viewing a webpage of Google search results, the user would be directed to the home page of Apple Inc., this being www.apple.com. (There is a list of 170 such keywords, associated with about twenty third-party merchants, further discussed

[6] See Cmpl. ¶ 19.
[7] Cmpl. ¶¶ 20-22.
[8] Paxfire was contracted by ISPs to improve their users' Internet experiences. For example, instead of receiving an error page when typing an incorrect address or "url" into an address bar on a web browser, Paxfire could return to the user's computer screen a web page offering suggestions as to where the user intended to go or other placers the user might want to visit.

below.) If directed to such a web page for a third-party merchant (as is true for any web page visited by a user, whether or not Paxfire was involved) a record of that visit was created and kept in files located on the computer's hard drive, which files maintained the user's browsing history.

To disprove Ms. Feist's claims, Paxfire would have used the absence of Paxfire's cookie on her computer to establish that it was not involved in the transmission of Ms. Feist's internet communications (and if it was so involved, to limit when it was involved by examining the date that cookie was placed on that computer); and would have used the absence of any records, that Ms. Feist visited any third-party merchants to which Paxfire may have redirected users, to show that Paxfire did not redirect her communications (and if it did so redirect, then to limit the number of such redirections by examining to where and when they occurred). The records needed to do this were on the hard drive of Ms. Feist's personal computer.

Ms. Feist destroyed this evidence after she filed her lawsuit.

**II. Ms. Feist Destroyed Material Evidence**

Paxfire's then-codefendant, RCN, served a Request for the Production of Documents ("RFP"), dated February 6, 2012, including a request for "Each Device that Ms. Feist has used since January 1, 2007 to access the Internet, or a copy of the hard drive of each such Device." (Exhibit 1, RCN RFP No. 12). By means of its own RFP, dated February 23, 2002, Paxfire made the identical request. (Exhibit 2, Paxfire RFP No. 10.)

Ms. Feist refused to produce the relevant drive or a copy. (Exhibit 3, Feist Response to RCN RFP No. 12; Exhibit 4, Feist Response to Paxfire RFP No. 10.) Eventually, however, she agreed to comply with the Defendants' requests, surrendering two drives to a Mr. Michael Wudke, a forensic computer expert retained by RCN. (Decl. Wudke at ¶ 10, Exhibit 5.)

Michael Wudke is the president of TransPerfect Legal Solutions Digital Forensics Division ("TransPerfect"). Ms. Feist's representatives provided to him two hard drives: (1) a Memorex Portable hard drive; and (2) a Western Digital Portable hard drive. The Plaintiff's representatives told him the following:

> Plaintiff's representatives explained that Drive 1 contained data recovered from the Plaintiff's original hard drive by Secure Data Recovery ("SDR"), a third party data recovery vendor. Drive 2 was described by Plaintiff's representatives as the "original" drive from Plaintiff's Computer. TransPerfect advised Plaintiff's representatives that this was unlikely due to the type of drive and enclosure, and requested that Plaintiff's representatives provide clarification as to the drive's origin. Plaintiff's representatives later stated that Drive 2 was believed to be a backup drive belonging to Plaintiff, not the "original" drive as was previously put forth.

(Decl. Wudke at ¶ 13.)

Mr. Wudke and TransPerfect conducted a forensic examination of the two hard drives, looking for, among other things, cookies and website cache files, and browser ("url") histories. (Decl. Wudke at ¶ 18.). Among his conclusions were:

(1) Standard Windows Operating System folders were missing on both drives. These folders store many of the types of files that are informative as to how the computer was used, including Internet searching and browsing habits. (Decl. Wudke at ¶ 15.)

(2) He found no records of web ("url") addresses having dates prior to March 2012; and none of the other records on these drives provided any evidence of Ms. Feist's "Internet searching or browsing habits prior to March 2012. (Decl. Wudke at ¶ 18.)

(3) The second hard drive contained files indicating the installation of a "cleaning" program, specifically Piroform's CCleaner ("CCleaner"). As explained by Mr. Wudke, "Applications such as CCleaner are commonly used to delete caches and files related to Internet searching and browsing," and "The presence of CCleaner on [Ms. Feist'] Computer, and [her]

use of same, may explain the absence of Internet history records prior to March 2012." (Decl. Wudke at ¶ 19.)

Ms. Feist was deposed twice in this case. The second deposition took place on August 17, 2012. During that deposition, Ms. Feist admitted that she used CCleaner to destroy to the cookies and browsing history stored on her computer:

> Q: [B]y your statement that you may have allowed evidence in your possession identifying the web pages you visited prior to March 16, 2012 to be deleted, are you referring to running CCleaner?
>
> A: Yes, I'm referring to running CCleaner. I can't think of anything that I know of other than that. But, you know, errors happen on computers too, you know.
>
> Q: And when you -- did you run the CCleaner program after the filing of your complaint?
>
> A: Yes.
>
> Q: And you intentionally ran that program, correct?
>
> A: I intentionally ran that program, but not intentionally to destroy evidence. I intentionally ran that program as part of my computer maintenance.
>
> Q: When you ran that program after the filing of your complaint, were you aware that it would delete your Internet browsing history?
>
> A: Yes and no. I mean, I had it set up so it would do that and -- but I didn't think about it.
>
> Q: So is it fair to say that you were aware that CCleaner would delete your browsing history, but you didn't run the program with the specific intent of deleting your browser history?
>
> A: Yes. Yeah, I guess that comes pretty close.

(2nd Dep. B. Feist at 370:6-371:19, Exhibit 6.)[9]

[9] The Errata Sheet of Ms. Feist, signed under oath and adopting and authenticating the deposition, is Exhibit 7.

She also admitted, during her first deposition which took place on April 13, 2012, that she used CCleaner to erase cookies stored on her computer as well as to erase her browsing history:

> Q: Do you make any effort to delete the browser history for your Internet browsers
>
> A: I use this CClean Program to delete cookies and various other things periodically, yes.

(1st Dep. B. Feist at 173:2-7, Exhibit 9.)

Put simply, after she filed her Complaint, after making her claims against Paxfire, she destroyed the very evidence that Paxfire could use to dispute her claims that Paxfire intercepted her electronic communications and redirected her electronic searches.

## III. This Court May Fashion a Remedy for Feist's Spoliation Under Both Rule 37(e) and Its Own Inherent Power

"A party has a duty to retain evidence that it knows or reasonably should know may be relevant to pending or future litigation." *Barsoum v. NYC Housing Authority*, 20 F.R.D. 396, 400 (S.D.N.Y. 2001)(J. Sweet), *citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998).*

Here, Ms. Feist had a duty to preserve the evidence of her internet searches that were on her personal computer: she brought the case against Paxfire, and she had counsel at the time that she brought the case. She is not pedestrian user of computers: she wrote two books about computers, and took programing courses at Baruch College. (1st Dep. Feist at 14:24–16:21, Exhibit. 9.) She "knew or should have known" that her search history would be relevant to the litigation that she commenced. *Barsoum* at 400. Yet, she destroyed important, material evidence, prejudicing Paxfire in the process.

Federal Rule 37(e) addresses how the courts should treat the spoliation of electronically stored evidence. It was amended effective December 1, 2015, and now reads:

> **(e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION.** If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Rule 37(e) addresses a party's failure to "take reasonable steps to preserve" electronically stored information. However, Ms. Feist did not simply fail to take reasonable steps to preserve her cookies and internet browser history—Ms. Feist's conduct is worse: she willfully erased this information. Paxfire analyzes the issues presented by this motion under both Rule 37(e) and the separate, inherent power of this Court to impose sections for the willful destruction of evidence. See *Erickson v. Kaplan Higher Educ., LLC*, 2015 U.S. Dist. LEXIS 142789, at *19 n. 6 (D. Md. Oct. 21, 2015) (discussing, prior to its effective date, remedies available under the amended version of Rule 37(e)).

A. Spoliation and the Inherent Powers of this Court

Spoliation and the imposition of remedies and sanctions for such conduct were discussed in significant detail by the court in *Ceglia v. Zuckerberg*, 2013 U.S. Dist. LEXIS 45500 (W.D.N.Y. Mar. 26, 2013):

> "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Company*, 167 F.3d 776, 779 (2d Cir. 1999) (citing *Black's Law Dictionary* 1401 (6th ed. 1990)). Sanctions for spoliation of evidence may be imposed either under Fed.R.Civ.P. 37(b) when the spoliation occurs in violation of a court order, *id*. (citing Fed.R.Civ.P. 37(b)(2); *John B. Hull, Inc. v. Waterbury Petroleum Prods. Inc*., 845 F.2d 1172, 1176 (2d Cir. 1988)), or pursuant to the court's inherent power to control litigation. *Id*. (citing *Chambers v. Nasco*, 501 U.S. 39, 43-45 (1991); *Sassower v. Field*, 973 F.2d 75, 80-81 (2d Cir. 1992)). The proper sanction for spoliation "should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine." Id. (citing *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998)). Ideally, a spoliation sanction should be designed to: (1) deter spoliation; (2) place the risk of an erroneous judgment resulting from the spoliation on the party who engaged in the spoliation; and (3) "restore 'the prejudiced party to the same position he would have been in absent the wrongful destruction of evidence by the opposing party.'" *Id*. (citing and quoting *Kronisc*h, 150 F.3d at 126).
>
> Nevertheless, "outright dismissal of a lawsuit . . . is within the court's discretion." *West*, 167 F.3d at 779 (quoting *Chambers*, 501 U.S. at 45). "Dismissal is appropriate if there is a showing of willfulness, bad faith, or fault on the part of the sanctioned party." *Id*. (citing *Jones v. NFTA*, 836 F.2d 731, 734 (2d Cir. 1987)). Dismissal, however, being an extreme sanction, "'should be used only in extreme circumstances, usually after consideration of alternative, less drastic sanctions.'" *Id*. (quoting *John B. Hull, Inc*., 845 F.2d at 1176).

*Id*. at *189-192.

The nature of the remedy imposed for spoliation rests upon the "level of intentionality" of the guilty party. *Barsoum* at 400. Dismissal requires a showing of "willfulness, bad faith, or any fault" on the part of the sanctioned party. "Fault" includes gross negligence. *Id.* A showing of bad faith is not a prerequisite for the imposition of sanctions under the inherent powers of the Court: willfulness or fault is enough. *Vodusek v. Bayliner Marine Corp*., 71 F.3d 138, 156 (4th Cir. 1995) (discussing adverse inference), citing *Glover v. BIC Corp*., 6 F.3d 1318, 1329 (9th Cir. 1993).

In the Second Circuit, the standard for the imposition of sanctions is fairly low: an adverse inference instruction—informing the jury that it may presume that evidence destroyed

was adverse to the party responsible for its preservation—could be imposed upon a finding of ordinary negligence. The rationale behind this holding is that party is responsible for the risk to its own evidence. *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2nd Cir. 2002).

B. Rule 37(e)

The newly amended version of Rule 37(e) broadens the statutory authority of a Court to impose remedies for the spoliation of electronically stored evidence: it is no longer necessary for a party to first violate a court order regarding production of the evidence in order to be liable for sanctions. Mere failure to "take reasonable steps to preserve" such evidence may be sanctioned. However, the rule limits the authorization for a Court to dismiss the guilty party's claims, give an adverse inference instruction to a jury, or otherwise presume that the evidence lost would have been favorable to the opposing party: such remedies are authorized where a party's failure "to take reasonable steps to preserve" was done intending to deprive another party of the use of the evidence. Fed. R. Civ. P. 37(e)(2). Without such a finding, the Court is authorized to take steps "no greater than necessary" to cure any prejudice to the affected party.

## IV. Paxfire Has Suffered Prejudice and Is Entitled to Sanctions

In *Erickson v. Kaplan Higher Educ., LLC*, 2015 U.S. Dist. LEXIS 142789 (D. Md. Oct. 21, 2015), the district court found spoliation in a very similar circumstance to what occurred here, imposing sanctions where a party willfully destroyed evidence:

> I do find, however, that even accepting Plaintiff's version of events, she acted willfully in that she acknowledged potentially relevant evidence was contained on her computer and nonetheless ran a program that she knew would destroy some data. That is, spoliation, "though not conducted in bad faith, could yet be 'intentional,' 'willful,' or 'deliberate.'" Plaintiff's willful state of mind could

> justify an adverse inference about Plaintiff's consciousness of the weakness of her case.

*Id*. at *16 (citations omitted).

As we now discuss, Ms. Feist's conduct was willful and demonstrated bad faith.

Her conduct was willful: she installed and then *manually* ran CCleaner, knowing that it would delete her browsing history. She ran CCleaner *after* she filed her lawsuit (2nd Dep. Feist at 370:15), doing so despite being told by her attorneys of her "document preservation obligations." (Aff. B. Feist at ¶ 5, Exhibit 8.) And she did not back-up or otherwise preserve her cookies or search history before erasing this evidence. (*Id*. at ¶ 5; 2nd Dep. Feist at 376:13 – 379:20.)

Given Ms. Feist's computer background, the instructions given to her by her attorneys, and her decision to bring her claims against Paxfire based upon her use of her own computer—her destruction of this material evidence cannot be said to be mere negligence or inadvertence: it is willful destruction of evidence.

Further, Ms. Feist demonstrated bad faith during discovery.

She first produced an affidavit wherein she said that she "may have run CCleaner after commencement" of her lawsuit. (Aff. Feist ¶ 5). Then, in her deposition, she conceded that there was no "may" about it: she definitely ran CCleaner, doing so after she filed her lawsuit. (2nd Dep. Feist at 370:15-18.)

After a lengthy discovery dispute among the parties, her attorneys produced two hard drives. (Decl. Wudke at ¶¶ 11-13.) They represented that the second of the two ("Drive 2") was the original hard drive from Ms. Feist's computer. (*Id*. at ¶ 13.) However, *neither was in fact from Ms. Feist's computer*: when presented with the evidence that the second drive and its enclosure did not match what was used on the type of computer that Ms. Feist owned, they

conceded that Drive 2 "was believed to be the backup drive belonging to" Ms. Feist, and not the "original" drive as represented. (*Id.*)

*To-date, Ms. Feist has never produced her original drive for examination in discovery*. A letter dated April 20, 2012 from RCN's counsel, Derek Care, to Ms. Feist's counsel, documents that Ms. Feist's hard drive supposedly "crashed" while it was being copied for discovery purposes. (Letter from D. Care to P. Seidman and K. Richman, April 20, 2012, at Pt. 4, Exhibit 10.) There remain open questions as to whether the original drive exists, where it is located, and its functioning condition.

In summary: (1) Ms. Feist had the relevant hard drive in her possession at the time she commenced this litigation; (2) she made no copy of her cookies or search history, on her computer's hard drive, prior to, or at the time that, or shortly after she filed the lawsuit so as to preserve her cookies and search history; (3) after she filed her lawsuit, she manually destroyed the records of her cookies and search history using the CCleaner application; (4) she (through her attorneys) represented that she was producing the original drive, from her personal computer, for examination in discovery, which was false; (5) she has never produced the original of her hard drive, giving no explanation as to why it has been withheld; and (6) the evidence she destroyed would have enabled Paxfire to demonstrate that Paxfire did not intercept her communications and did not redirect any of her internet searches.

Ms. Feist has willfully destroyed evidence; and she has demonstrated bad faith regarding this destruction, through her false statement that she produced her original hard drive and her continued failure to produce this drive.

## V. Count One of Ms. Feist's Complaint Should be Dismissed—Alternatively, Any Evidence as to Interception and Redirection by Paxfire Should Be Ruled Inadmissible

We note that Ms. Feist does not allege that Paxfire redirected all of her internet searches, but only certain keywords found on a list of some 170 search terms. This list is attached as Exhibit 11. (2nd Dep. Feist 313:12-315:13, citing Exhibit 20 to the deposition (Exhibit 11 to this motion).) We further note that Ms. Feist does not claim that Paxfire redirected these keywords each time she entered one into the search bar of her browser (1st Dep. Feist at 93:18-94:10); nor does she know how many times she entered any word found in the keyword list into a search bar and was (supposedly) redirected. (1st Dep. Feist at 95:17-95:25.) In fact, *she cannot remember any name* that she entered into a search bar that was in fact redirected. (1st Dep. Feist at 95:2-9.)[10]

The only evidence that once existed that Paxfire intercepted, redirected, or disclosed any of Ms. Feist's search terms was stored in the cookies and her search history on her computer's hard drive—and she destroyed that evidence.

For the reasons discussed, Ms. Feist must be sanctioned for the spoliation of material evidence. The appropriate sanction is dismissal of Count One of her Complaint, which relies exclusively on the interception and redirection of specific electronic communications—which

[10] The best that Ms. Feist could do in this regard was to testify that she "might" have been redirected when she entered the word "apple" into a search engine. But she then clarified this, while looking at the keyword list, by adding that she didn't think so, because she would not have entered merely the word "apple," but would have entered a term dealing with apples, such as apple recipes, or sources of apples (which are not on the list): "[I] don't know. That's the only word on this list offhand that I can think of that I wouldn't either be interested in the [trademark's] corporate information or wanting to reach the [the trademark owner's] website." (2nd Dep. Feist at 326:19-327:19.) She had no specific recollection of having been redirected while searching for apple as a generic term. (*Id*. at 327:14-19.) She also said she might have looked for "cheap flights," but had no recollection that she did. (*Id*. at 327:18-328:18.)

she (allegedly) transmitted to and through her ISP (Cmpl. ¶¶ 45-47).[11] Without this remedy, Paxfire will be at risk of liability where Ms. Feist's willful conduct prevents Paxfire from disputing specific instance where she may claim her communications were intercepted or redirected. This will include how many such instances there were, to which third-party merchants she may have been redirected, and during what period of time these interceptions or redirections supposedly occurred. She alleges each instance as a separate violation, and seeks statutory penalties for each instance in addition to actual damages and attorneys' fee. (Cmpl. ¶ 49.) *See Ceglia* at *240 (spoliation of evidence as alternate basis for granting motion to dismiss).

In the alternative, Ms. Feist must not be allowed to introduce at trial, or during motion practice for summary judgment, any evidence that Paxfire intercepted any specific electronic communication or redirected any specific internet search made by her. No introduction by Ms. Feist of any evidence—whether directly or by inference, and whether through her own testimony, through an expert, or by any other means—should be admitted for the purpose of establishing that Paxfire intercepted any of her electronic communications, or that she conducted internet searches using any of these 170 keywords. *Erickson* at *17-18 (recommending the preclusion of documentary evidence which could not be authenticated due to plaintiff's misconduct).

[11] Paxfire is also named in Counts Four and Five of her Complaint. Paxfire does not with this motion seek the dismissal of these counts. Although Count Three uses the phrase "Defendants" in its charging language, Ms. Feist confirmed before District Judge Koeltl that this count does not address the conduct of Paxfire. (Transcript of Hr'g, Jan. 31, 2012, at 20-21, Doc. 49.)

## CONCLUSION

For the reasons set forth above, Count One of Ms. Feist must be dismissed with prejudice. In the alternative, any evidence as to specific instances of Paxfire intercepting Ms. Feist's electronic communications or redirecting her internet searches must be ruled inadmissible for the purposes of trial and summary judgment motions.

Dated: December 10, 2015

Respectfully submitted,

/s/ Andrew Grosso
Andrew Grosso, Esq.
ANDREW GROSSO & ASSOCIATES
Georgetown Place
1101 Thirtieth Street, NW, Suite 300
Washington, DC 20007
Tel.: 202-298-6500
Fax: 202-298-5499
Email: agrosso@acm.org

*Counsel for Defendant−Counterclaim Plaintiff Paxfire, Inc.*

**EXHIBIT LIST**

1. RCN's First Request for Production of Documents, February 6, 2012

2. Paxfire's First Request for Production of Documents, February 23, 2012

3. Feist's Response to RCN's First Request for Production of Documents, March 7, 2012

4. Feist's Response to Paxfire's First Request for Production of Documents, March 26, 2012

5. Expert Declaration of Michael Wudke, October 11, 2012

6. 2nd Deposition of Betsy Feist, August 17, 2012 (Excerpts)

7. Errata Sheet to 2nd Deposition of Betsy Feist, October 3, 2012

8. Affidavit of Betsy Feist, July 1, 2012

9. 1st Deposition of Betsy Feist, April 13, 2012 (Excerpts)

10. Letter from D. Care to P. Seidman and K. Richman, April 20, 2012

11. Paxfire Keyword List, Exhibit 20 to 2nd Deposition of Betsy Feist

12. Deposition of Michael Sullivan, August 2, 2012 (Excerpts)

**CERTIFICATION OF SERVICE**

I certify that on this 10th day of December 2015, I caused this paper to be served on all counsel of record by email through the ECF system pursuant to the Federal Rules of Civil Procedure and the Local Rules.

/s/Andrew Grosso
Andrew Grosso